Guidance for Insurance Sector on the Best Practices for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Compliance

Approved by FSC Letter No. Jin-Guan-Bao-Zong-Zi-10704937560 dated July 24, 2018

Foreword:
These best practices guidance is provided for the reference of insurance enterprises in undertaking anti-money laundering and combating the financing of terrorism (AML/CFT) operation. It is not meant to be mandatory. An insurance enterprise may, based on the nature and size of its business and in consideration of the results of risk assessment in the areas of geographic locations, customers, products and services, transactions and delivery channels, select the most appropriate best practices to prevent or reduce money laundering and terrorist financing (ML/TF) risks.

1. Suspicious transaction reporting

(1) Enhance the effectiveness of monitoring suspicious ML/TF transactions

For the detection of unusual transactions, an insurance company should refer to the red flags for money laundering or terrorism financing transactions set out by the insurance association, and in addition, signs of suspicious activities set by the company itself based on its past experience, and employ information system and manual check in the detection.

(2) Suggestions for evaluating suspicious transactions

1) Consider the situation of individual customers when evaluating the reasonableness of a customer's activities and keep relevant inspection records.

2) If a customer transaction is suspected of money laundering or terrorist financing following evaluation, the insurance company is advised, after filing a STR with the Investigation Bureau, Ministry of Justice (MJIB), to adjust the risk rating of the reported customer to high risk to facilitate the system's automatic screening of high-risk customers for subsequent transactions.

3) If a customer transaction is deemed not suspicious following evaluation, the insurance company should still record the evaluation result and reason for exclusion.

(3) Suggestions for enhancing reporting quality and the thoroughness of report

1) Reasons for filing a STR should cover who, what, when, where, and how. For example, customer identity (background and occupation), and specific irregularities of the unusual transaction (date, amount, transaction frequency or cycle, etc.)
2) Provide comprehensive supporting information, for example, insurance policy, transaction details or fund transfer details on the unusual transaction.
3) Communicate and interact fully with the MJIB by, for example, periodically following up on the status of reported cases (under analysis, forwarded to prosecutor's office or put under reference data for the time being) to learn whether the reported data are comprehensive.
4) Periodically analyze and review the patterns and types of suspicious transactions. For example, connection with the types of predicate offences for money laundering, the ratio of numbers of actual STR filed to the number of company-wide suspicious transactions under monitoring, and evaluate the reasonableness of the percentage to learn whether there is defensive reporting or whether the conditions set for monitoring are too stringent, and feedback the evaluation findings in a timely manner to adjust the company's reporting rules.

(4) Suggestions for enhancing employees' ability to identify ML/TF risks

To increase the alertness of front-line staff to signs of suspicious transactions and enhance the quality of STR, an insurance company can hold training courses for employees to help them understand matters to pay attention to in filing a STR, promote the importance of suspicious transaction monitoring, and analyze the types of STR filed by the company in the past

(5) Suggestions for preventing the leak of STR information

1) Employees at all levels must keep confidential related data of transactions reported to MJIB unless otherwise authorized to disclose.
2) Related data of reported transactions (e.g. loan repayment details, insurance application, etc.) transmitted via internal email should be encrypted.
3) Dedicated Unit Officer should authorize the designated personnel to handle

suspicious transaction reporting.

4) Paper official documents sent to MJIB should be classified confidential and delivered by certified mail.

5) When filing a STR via media:

A. Filing of a STR must first be approved by the Dedicated Unit Officer or an officer authorized by him/her.

B. IC card and password used for online filing should be kept by different staff.

C. There should be access control in place when the designated personnel files STR via media.

2. Record keeping of transactions involving high-risk products

(1) Factors to be considered in identifying high-risk products

An insurance company can use a risk-based approach to identify and assess types of products posing high ML/TF risk and should take corresponding risk mitigation measures. Risk factors to be considered in identifying and assessing high -risk products are exemplified below:

1) Degree of association with cash.

2) Does the product involve high premium or high cash value?

3) Is single premium allowed for the product?

4) Is a free-look period provided for policy?

5) Is a large number of transactions in a short period of time allowed?

6) The amount of policy surrender charge (high or low).

7) Are anonymous payments (e.g. premium payment or repayment of policy loan) or payments by unrelated third parties allowed?

8) Can the benefit or surrender value be paid to an unrelated third party?

9) Is cross-border receipt or delivery of payments allowed?

10) The channel to establish business relationships or delivery channel, including whether it is a face-to-face transaction or a new type of delivery channel, such as electronic commerce or transaction through the offshore insurance unit.

11) The degree of association with predicate offences.

(2) Factors to be considered in keeping transaction records of high-risk products

1) The feasibility of integrating insurance policy information by customer:

An insurance company should, if feasible, integrate all insurance policy information of individual customers to evaluate the degree of a customer's transactions involving high risk products.

2) Correlation of transaction records:

An insurance company should link up the transaction records of individual customers to get a holistic view of the customer's transaction pattern and history.

3) Possibility of reconstructing transaction records:

Transaction records should be kept in such a way as allows to reconstruct individual transactions, so that the records can present the holistic transaction process and content.

4) Immediate storage and access of transaction records:

Transaction records should be promptly stored and be readily accessible when needed to make sure records are swiftly available to competent authorities or law enforcement agencies upon request.

(3) Suggestions for the retention of transaction records of high-risk products

1) Retention period

Transaction records of high risk products should be kept for at least 5 years after business relationship with the customer ends, and the retention periods for different high risk products purchased by the customer should be taken into overall consideration. However, if a longer retention period is required as otherwise provided by law or as deemed necessary by the insurance company out of risk management consideration, the longer retention period prevails.

2) Contents of record

A. All records obtained in customer due diligence, e.g. copies or records of official identification documents like passport, identity card, driver's license or similar documents, copies or records of identification documents of customer or persons acting on behalf of

the customer, data or information of beneficial owners; customer's risk assessment and classification records, watch list filtering records, and other customer due diligence or enhanced due diligence records.

B. Contract documents and files, e.g. insurance provisions, attached application forms, endorsements and other agreements.

C. Business correspondence, e.g. inquiries to establish the background and purpose of complex, unusual large transactions and the results of any analysis undertaken, purpose and nature of business relationship, information on customer's source of wealth and sources of funds.

D. Necessary transaction information, e.g. name, or account number or identifier of each party involved in a transaction, date of transaction, currency and amount of transaction, the way payments are made or delivered (e.g. cash, checks), destination of funds, and ways to provide instructions or authorization.

E. Transaction monitoring records, e.g. records of approvals given by senior management based on the approval hierarchy set by the insurance company in consideration of internal risks, records of ongoing transaction monitoring, and records of enhanced ongoing monitoring during the course of business relationship.

3) Retention methods

For transactions involving high risk products, an insurance company can keep business correspondence and customer transaction records in hard copy or electronic form in such a way that it will permit reconstruction of individual transactions. An insurance company should also consider the security of stored documents and electronic data that they can be used as evidence for prosecution of criminal activities.

4) When an insurance company engages a third party assist in customer due diligence, appropriate measures for the preservation of records by third parties should be considered .

3. Managing terrorist financing (TF) risks

(1) To effectively enhance the management of TF risks, an insurance company can consider the following actions:

1) Establish an AML/CFT program and implement a training program:

An insurance company should establish an AML/CFT program and carry out employee training on AML/CFT compliance.

2) Grasp TF threats and trends:

A. Watch closely negative news reports on terrorist financing and grasp timely international trends on combating terrorist financing.

B. Keep abreast of the trend of terrorist organizations raising funds through legal sources or non-profit organizations.

C. Keep abreast of how terrorist organizations using new technologies to raise and transfer funds.

3) Keep up with the sanction lists:

Visit constantly the AML/CFT webpage of the Ministry of Justice, which has a sanction lists section and allows subscription of electronic notice of updated sanction lists, and pay attention to the updates of sanction lists.

4) Build a sanction list database:

An insurance company should not use the externally purchased database as the only source for sanction lists, and is advised to also build its own sanction list database. Upon learning or receiving a list of designated individuals or entities, the company should check if it has been included in the externally purchased database. If not, key it into its own list database. Terrorists or terrorist groups identified or investigated by foreign governments or international organizations should be included in the scope of data to be collected by the database, and the insurance company should pay attention to related transaction risk.

5) Identify and restrict transactions:

Before establishing business relationship or carrying out a transaction with a customer, an insurance company should identify customer identity. If a customer is confirmed to be on the list of designated individuals or entities, the insurance company may not establish business relationship, nor carry

out any transaction with the customer, unless it is otherwise permitted by the TF Review Committee.

6) Freeze assets and make a report:

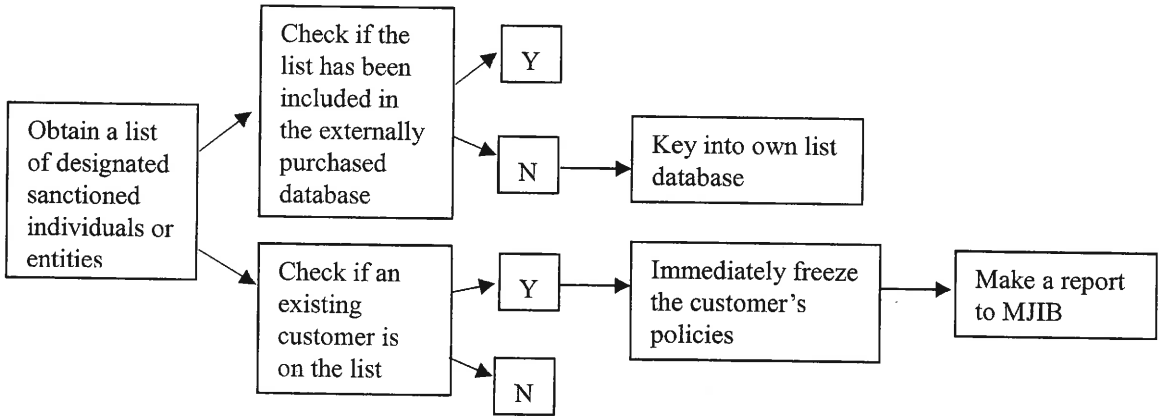
Upon learning or receiving a list of designated individuals or entities, an insurance company should check swiftly if any existing customer is on the list. If yes, the company should immediately freeze the customer's policies and file a report with MJIB in 10 business days upon discovery.

7) Keep related information confidential:

Relevant personnel who learn through business the reporting of properties or property interests and locations of designated sanctioned individuals or entities to MJIB should keep the reporting information confidential.

(2) Suggestions for combating the financing of terrorism (CFT) procedure:

1)



2)